Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method for carrying out an electronic transaction across a communication network linking several entities~~; this method is characterised in that~~ comprising the following steps:

a) a first entity builds a first message combining ~~all of the~~ transaction data and calculates a first cryptogram of ~~this~~ said first message using a first key system that [[it]]said first entity shares with [[the]]a last (n^{th}) entity; ~~this~~ said first entity then links a second message with [[the]]said first cryptogram and calculates a second cryptogram of ~~the whole~~ said second message linked with said first cryptogram using a second key system that [[it]]said first entity shares with ~~the last but one~~ an $(n-1)^{th}$ entity, and so on; [[the]]said first entity links an $(n-1)^{th}$ message with [[the]]an $(n-2)^{th}$ cryptogram previously obtained and calculates an $(n-1)^{th}$ cryptogram of ~~the whole~~ said $(n-1)^{th}$ message linked with said $(n-2)^{th}$ cryptogram using [[the]]an $(n-1)^{th}$ key system that [[it]]said first entity shares with [[the]]a second entity; [[the]]said first entity then sends [[the]]a last

calculated cryptogram across the communication network;

b) [[the]]said second entity receives ~~this~~ said last cryptogram, uses [[the]]an appropriate key system to extract [[this]]said $(n-1)^{th}$ message from [[the]]said $(n-1)^{th}$ cryptogram containing [[it]]said $(n-1)^{th}$ message, and sends [[the]]said remaining $(n-2)^{th}$ cryptogram to [[the]]a third entity, and so on; [[the]]said n^{th} entity receives [[the]]said first cryptogram and uses [[the]]an appropriate key system to extract [[the]]said first message contained within [[it]]said first cryptogram.

Claim 2 (original): A method in accordance with claim 1, whereby the communication network therefore only includes entities that share a key with a first entity; the transaction then takes place between this first entity, which is the message source, and the last entity, which is the message recipient.

Claim 3 (original): A method in accordance with claim 1, whereby the communication network includes a first group of entities made up of a first entity and (i-1) others, each of which shares a key system with said first entity, and a second group of entities made up of a first entity that is the last entity of this first group, i.e. entity i,

and (n-i) others, and whereby entity i shares a key system with each of the (n-1) following entities, said method being made up of two successive stages:

a first stage, in which the message built by the first entity of the first group is sent to the i^{th} entity of the first group in accordance with operations a) and b) in claim 1;

a second stage, in which the message extracted by the first entity of the second group is sent to the last entity of the second group in accordance with said operations a) and b) in claim 1.

Claim 4 (original): A method in accordance with claim 1, whereby the communications network is composed of a first group of entities made up of a first entity and (i-1) others that share a key system with said first entity, a second group of entities made up of a first entity that is the last entity of this first group and (j-i+1) others that share a key system with said first entity of this second group, a third group of entities made up of a first entity that is the last entity of said second group and (n-j) others, where the (n-j+1) entities of this third group share a key system with said first entity of the first group, this method being characterised in that:

the first entity of the first group performs operations a) set forth in claim 1, using the key systems

that it shares with all other entities in the first and third groups;

the entities in the first group process the cryptograms that they receive in accordance with operations b) set forth in claim 1;

the first entity of the second group performs operations a) set forth in claim 1, using the key systems that it shares with all other entities in this second group;

the entities in the second group process the cryptograms that they receive in accordance with operations b) set forth in claim 1;

the entities in the third group unencrypt the cryptograms that they receive in accordance with operations b) set forth in claim 1.

Claim 5 (original): A method in accordance with claim 1, whereby a group's first entity, i, calculates a cryptogram of the messages intended for the group's other entities, i+1, i+2, ..., j, without encapsulating them, and whereby each entity i+1, i+2, ..., j receives and checks the message intended for it using its key system that it shares with i.

Claim 6 (original): A method in accordance with claim 1, whereby the electronic transaction is a payment and whereby the entities are composed of cards (A), service points (P) capable of receiving said cards (A), service point concentrators equipped with a security module (MS) and connected to the service points and an issuer (E) responsible for issuing electronic payment cards and obtaining the electronic money, the communication network connecting service points (P) with the concentrators and said concentrators with the issuer, whereby each card (A) shares a key system $K_{A,M}$ with a security module (MS), whereby each card A also shares a key system $K_{A,E}$ with the issuer (E), and whereby each card (A) shares a key system $K_{A,P}$ with a service point (P).

Claim 7 (original): A method in accordance with claim 6, in which:

a) the card (A):

calculates a message (M') intended for the issuer (E), whereby said message contains the running total of the amounts paid, the transaction number (NT_A), the transaction number (NT_{MS}) of the security module (MS) to which the service point is connected and the identifier of said security module (ID_{MS}),

calculates a first cryptogram $K_{A,E}(M')$ of said message using key system $K_{A,E}$ that it shares with the issuer,

adds a message (M) containing the transaction amount (m), running total, transaction numbers (NT_A, NT_{MS}) and identifier (ID_{MS}) to said first cryptogram,

encapsulates the result in a second cryptogram $K_{A,M}(M, K_{A,E}(M'))$ using key system $K_{A,M}$ that it shares with the security module (MS),

adds message M to said second cryptogram,

encapsulates the result in a third cryptogram $K_S(M, K_{A,M}(M, K_{A,E}(M'))$ using key system $K_{A,P}$,

sends said third cryptogram to the service point (P),

b) said service point (P) uses key system $K_{A,P}$ to decapsulate the cryptogram that it has received, retrieves and checks message M and records $K_{A,M}(M, K_{A,E}(M'))$, and whereby the method is repeated if use of the service has not ended,

c) when the service session ends the service point (P) resends the last message $K_{A,M}(M, K_{A,E}(M'))$ to the security module (MS),

d) said security module (MS) uses key system $K_{A,M}$ to decapsulate the cryptogram that it has received, retrieves the message (M) and sends $K_{A,E}(M')$ to the issuer,

e) said issuer (E) uses key system $K_{A,E}$ to decapsulate the cryptogram that it has received and extracts the message (M') intended for it.